

Department of the Army, DoD

Pt. 505, App. H

release to that activity. Do not use general statements, such as "To other federal agencies as required" or "To any other appropriate federal agency".

(j) *Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:*

(k) *Storage:* State the medium in which DA maintains the records; for example, in file folders, card files, microfiche, computer, or a combination of those methods. Storage does not refer to the storage container.

(l) *Retrievability:* State how the Army retrieves the records; for example, by name, fingerprints or voiceprints.

(m) *Safeguards:* Identify the system safeguards; for example, storage in safes, vaults, locked cabinets or rooms, use of guards, visitor controls, personnel screening, computer systems software, and so on. Describe safeguards fully without compromising system security.

(n) *Retention and Disposal.* State how long AR 25-400-2 requires the activity to maintain the records. Indicate when or if the records may be transferred to a Federal Records Center and how long the record stays there. Specify when the Records Center sends the record to the National Archives or destroys it. Indicate how the records may be destroyed.

(o) *System Manager(s) and Address:* List the position title and duty address of the system manager. For decentralized systems, show the locations, the position, or duty title of each category of officials responsible for any segment of the system.

(p) *Notification Procedures:* List the title and duty address of the official authorized to tell requesters if their records are in the system. Specify the information a requester must submit; for example, full name, military status, SSN, date of birth, or proof of identity, and so on.

(q) *Record Access Procedures:* Explain how individuals may arrange to access their records. Include the titles or categories of officials who may assist; for example, the system manager.

(r) *Contesting Records Procedures:* The standard language to use is "The Army's rules for accessing records, and for contesting contents and appealing initial agency determinations are contained in Army Regulation 25-71; 32 CFR part 505; or may be obtained from the system manager."

(s) *Record Source Categories:* Show categories of individuals or other information sources for the system. Do not list confidential sources protected by 5 U.S.C. 552a(k)(2), (k)(5), or (k)(7).

(t) *Exemptions Claimed for the System:* Specifically list any approved exemption including the subsection in the Act. When a system has no approved exemption, write "none" under this heading.

APPENDIX G TO PART 505—MANAGEMENT CONTROL EVALUATION CHECKLIST

(a) *Function.* The function covered by this checklist is DA Privacy Act Program.

(b) *Purpose.* The purpose of this checklist is to assist Denial Authorities and Activity Program Coordinators in evaluating the key management controls listed below. This checklist is not intended to cover all controls.

(c) *Instructions.* Answer should be based on the actual testing of key management controls (e.g., document analysis, direct observation, sampling, simulation, other). Answers that indicate deficiencies should be explained and corrective action indicated in supporting documentation. These management controls must be evaluated at least once every five years. Certificate of this evaluation has been conducted and should be accomplished on DA Form 11-2-R (Management Control Evaluation Certification Statement).

TEST QUESTIONS

a. Is a Privacy Act Program established and implemented in your organization?

b. Is an individual appointed to implement the Privacy Act requirements?

c. Are provisions of AR 25-71 concerning protection of OPSEC sensitive information regularly brought to the attention of managers responsible for responding to Privacy Act requests and those responsible for control of the Army's records?

d. When more than twenty working days are required to respond, is the Privacy Act requester informed, explaining the circumstance requiring the delay and provided an appropriate date for completion.

e. Are Accounting Disclosures Logs being maintained?

Comments: Assist in making this a better tool for evaluating management controls. Submit comments to the Department of Army, Freedom of Information and Privacy Division.

APPENDIX H TO PART 505—DEFINITIONS

FUNCTION

(a) *Access.* Review or copying a record or parts thereof contained in a Privacy Act system of records by an individual.

(b) *Agency.* For the purposes of disclosing records subject to the Privacy Act, Components of the Department of Defense are considered a single agency. For other purposes including access, amendment, appeals from denials of access or amendment, exempting systems of records, and recordkeeping for release to non-DOD agencies, the Department of the Army is considered its own agency.

(c) *Amendment.* The process of adding, deleting, or changing information in a system

of records to make the data accurate, relevant, timely, or complete.

(d) *Computer Matching Agreement*. An agreement to conduct a computerized comparison of two or more automated systems of records to verify eligibility for payments under Federal benefit programs or to recover delinquent debts for these programs.

(e) *Confidential Source*. A person or organization who has furnished information to the Federal Government under an express promise that the person's or the organization's identity would be held in confidence or under an implied promise of such confidentiality if this implied promise was made before September 27, 1975.

(f) *Cookie*. A mechanism that allows the server to store its own information about a user on the user's own computer. Cookies are embedded in the HTML information flowing back and forth between the user's computer and the servers. They allow user-side customization of Web information. Normally, cookies will expire after a single session.

(g) *Defense Data Integrity Board*. The Board oversees and coordinates all computer matching programs involving personal records contained in systems of records maintained by the DOD Component; reviews and approves all computer matching agreements between the Department of Defense (DOD) and other Federal, State, and local governmental agencies, as well as memoranda of understanding when the match is internal to the DOD.

(h) *Disclosure*. The transfer of any personal information from a Privacy Act system of records by any means of communication (such as oral, written, electronic mechanical, or actual review) to any persons, private entity, or government agency, other than the subject of the record, the subject's designated agent or the subject's legal guardian. Within the context of the Privacy Act and this part, this term applies only to personal information that is a part of a Privacy Act system of records.

(i) *Deceased Individuals*. The Privacy Act confers no rights on deceased persons, nor may their next-of-kin exercise any rights for them. However, family members of deceased individuals have their own privacy right in particularly sensitive, graphic, personal details about the circumstances surrounding an individual's death. This information may be withheld when necessary to protect the privacy interests of surviving family members. Even information that is not particularly sensitive in and of itself may be withheld to protect the privacy interests of surviving family members if disclosure would rekindle grief, anguish, pain, embarrassment, or cause a disruption of their peace minds. Because surviving family members use the deceased's Social Security Number to obtain benefits, DA personnel should con-

tinue to protect the SSN of deceased individuals.

(j) *Individual*. A living person who is a citizen of the United States or an alien lawfully admitted for permanent residence. The parent or legal guardian of a minor also may act on behalf of an individual. Members of the United States Armed Forces are individuals. Corporations, partnerships, sole proprietorships, professional groups, businesses, whether incorporated or unincorporated, and other commercial entities are not individuals.

(k) *Individual Access*. The subject of a Privacy Act file or his or her designated agent or legal guardian has access to information about them contained in the Privacy Act file. The term individual generally does not embrace a person acting on behalf of a commercial entity (for example, sole proprietorship or partnership).

(l) *Denial Authority (formerly Access and Amendment Refusal Authority)*. The Army Staff agency head or major Army commander designated authority by this part to deny access to, or refuse amendment of, records in his or her assigned area or functional specialization.

(m) *Maintain*. Includes keep, collect, use or disseminate.

(n) *Members of the Public*. Individuals or parties acting in a private capacity.

(o) *Minor*. An individual under 18 years of age, who is not married and who is not a member of the Department of the Army.

(p) *Official Use*. Within the context of this part, this term is used when Department of the Army officials and employees have demonstrated a need for the use of any record or the information contained therein in the performance of their official duties.

(q) *Personal Information*. Information about an individual that identifies, relates, or is unique to, or describes him or her, e.g., a social security number, age, military rank, civilian grade, marital status, race, salary, home/office phone numbers, etc.

(r) *Persistent cookies*. Cookies that can be used to track users over time and across different Web sites to collect personal information.

(s) *Personal Identifier*. A name, number, or symbol that is unique to an individual, usually the person's name or SSN.

(t) *System of Records*. A group of records under the control of the DA from which information is filed and retrieved by individuals' names or other personal identifiers assigned to the individuals. System notices for all systems of records must be published in the FEDERAL REGISTER. A grouping of records arranged chronologically or subjectively that are not retrieved by individuals' names or identifiers is not a Privacy Act system of records, even though individual information could be retrieved by individuals' names or personal identifiers, such as through a paper-by-paper search.

(u) *Privacy Advisory*. A statement required when soliciting personally identifying information by a Department of the Army Web site and the information is not maintained in a system of records. The Privacy Advisory informs the individual why the information is being solicited and how it will be used.

(v) *Privacy Impact Assessment (PIA)*. An analysis, which considers information sensitivity, vulnerability, and cost to a computer facility or word processing center in safeguarding personal information processed or stored in the facility.

(w) *Privacy Act (PA) Request*. A request from an individual for information about the existence of, access to, or amendment of records pertaining to that individual located in a Privacy Act system of records. The request must cite or implicitly refer to the Privacy Act of 1974.

(x) *Protected Personal Information*. Information about an individual that identifies, relates to, is unique to, or describes him or her (e.g., home address, date of birth, social security number, credit card, or charge card account, etc.).

(y) *Records*. Any item, collection, or grouping of information, whatever the storage media (e.g., paper, electronic, etc), about an individual that is maintained by a DOD Component, including but not limited to, his or her education, financial transactions, medical history, criminal or employment history and that contains his or her name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

(z) *Records Maintenance and Use*. Any action involving the storage, retrieval, and handling of records kept in offices by or for the agency.

(aa) *Review Authority*. An official charged with the responsibility to rule on administrative appeals of initial denials of requests for notification, access, or amendment of records. Additionally, the Office of Personnel Management is the review authority for civilian official personnel folders or records contained in any other OMP record.

(bb) *Routine Use*. Disclosure of a record outside DOD without the consent of the subject individual for a use that is compatible with the purpose for which the information was collected and maintained by DA. A routine use must be included in the notice for the Privacy Act system of records published in the FEDERAL REGISTER.

(cc) *Statistical record*. A record in a system of records maintained for statistical research or reporting purposes and not used in whole or in part in making determinations about specific individuals.

(dd) *System Manager*. An official who has overall responsibility for policies and procedures for operating and safeguarding a Privacy Act system of records.

(ee) *Third-party cookies*. Cookies placed on a user's hard drive by Internet advertising networks. The most common third-party cookies are placed by the various companies that serve the banner ads that appear across many Web sites.

(ff) *Working Days*. Days excluding Saturday, Sunday, and legal holidays.

PART 507—MANUFACTURE AND SALE OF DECORATIONS, MEDALS, BADGES, INSIGNIA, COMMERCIAL USE OF HERALDIC DESIGNS AND HERALDIC QUALITY CONTROL PROGRAM

Subpart A—Introduction

Sec.

507.1 Purpose.

507.2 References.

507.3 Explanation of abbreviations and terms.

507.4 Responsibilities.

507.5 Statutory authority.

Subpart B—Manufacture and Sale of Decorations, Medals, Badges, and Insignia

507.6 Authority to manufacture.

507.7 Authority to sell.

507.8 Articles authorized for manufacture and sale.

507.9 Articles not authorized for manufacture or sale.

Subpart C—Commercial Use of Heraldic Designs

507.10 Incorporation of designs or likenesses of approved designs in commercial articles.

507.11 Reproduction of designs.

507.12 Possession and wearing.

Subpart D—Heraldic Quality Control Program

507.13 General.

507.14 Controlled heraldic items.

507.15 Certification of heraldic items.

507.16 Violations and penalties.

507.17 Procurement and wear of heraldic items.

507.18 Processing complaints of alleged breach of policies.

AUTHORITY: 10 U.S.C. 3012, 18 U.S.C. 701, 18 U.S.C. 702

SOURCE: 63 FR 27208, May 18, 1998, unless otherwise noted.